



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

✓-0

ELR

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
-----------------	-------------	----------------------	---------------------

08/927,382 09/12/97 COSS

M 1-1-1

EXAMINER

LM02/0926

JOSEPH B RYAN
RYAN AND MASON, L.L.P.
90 FOREST AVENUE
LOCUST VALLEY NY 11560

CROCKETT, R

ART UNIT

PAPER NUMBER

2785

DATE MAILED:

09/26/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

RA



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Paper No. 14

Application Number: 08/927,382
Filing Date: September 12, 1997
Appellant(s): COSS ET AL.

MAILED
SEP 25 2000
Group 2700

Coss et al.
For Appellant

EXAMINER'S ANSWER

This is in response to appellant's brief on appeal filed 12 July 2000.

(1) *Real Party in Interest*

A statement identifying the real party in interest is contained in the brief.

(2) *Related Appeals and Interferences*

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) *Status of Claims*

The statement of the status of the claims contained in the brief is correct.

(4) *Status of Amendments After Final*

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) *Summary of Invention*

The summary of invention contained in the brief is correct.

(6) *Issues*

The appellant's statement of the issues in the brief is correct.

(7) *Grouping of Claims*

Appellant's brief includes a statement that claims 1-26 do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

(8) *Claims Appealed*

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) *Prior Art of Record*

5,606,668

Shwed

2-1997

(10) *Grounds of Rejection*

The following ground(s) of rejection are applicable to the appealed claims:

Art Unit: 2785

Claims 1-26 are rejected under 35 U.S.C. 103(a). This rejection is set forth in prior Office Action, Paper No. 9.

(11) Response to Argument

Shwed (U.S. Patent 5,606,668) teaches or suggests each and every limitation of Applicant's independent claims 1, 8, 12, 17, and 22.

The Shwed system teaches a firewall.

As stated in previous Office Actions, Shwed teaches network security system comprised of packet filters (col. 3, lines 59-65; figs. 1, 2) installed on gateways, workstations, and other networking hardware. Packet filters were known by those in the art to be configurable software programs that could be installed on many types of hardware. It was well-known in the art, at the time the invention was made, that the term "firewall" used in the context of network security encompassed the term "network hardware supporting one or more packet filters," because network security firewalls functioned by blocking (filtering) undesirable message packets.

The "security policies" claimed by Applicant are not distinct from the security rules taught by Shwed.

A policy is ordinarily defined as "a definite course or method of action selected from among alternatives." Applicant's specification does not give any other special definition to this term. Therefore, one of ordinary skill in the art, at the time the invention was made, would have interpreted the term "security policy" as used in Applicant's claims to be indistinguishable from the term "security rule." This is because a "rule" in this context would have been recognized by one skilled in the art to be "a definite course or method of action selected from among alternatives."

Shwed teaches or suggests that his network security system can apply sets of security rules to packets.

Shwed discloses (col. 4, lines 17-26, fig.2):

...Each of the packet filters operates on a set of instructions which has been generated by the packet filter generator 208 in the system administrator 102. These instructions enable complex operations to be performed on the packet, rather than merely checking the content of the packet against a table containing the parameters for acceptance or rejection of the packet.

Art Unit: 2785

Thus, each packet filter can handle changes in security rules with great flexibility as well as handle multiple security rules without changing the structure of the packet filter itself.

Here, Shwed suggests to one of ordinary skill that his system can implement multiple security rules, and that a motivation for using multiple rules is increased flexibility.

Shwed teaches or suggests that his security system may extract all types of header data from layered protocol packets for use in matching packets with security rules.

Shwed discloses (col. 8, lines 38-49):

...The data extraction block 702 is shown in greater detail in FIG. 8. The process starts at block 802 and control passes to block 804 in which data is extracted from a specific address within the packet 806. This address is taken from the stack memory 618 or from the instruction code. The amount of data extracted is also determined by the stack memory or the instruction code. The extracted data is put into the memory stack 810 at block 808...

Shwed discloses (col. 6, lines 36-64):

...Different communication protocols employ different levels of the ISO model. A protocol in a certain layer may not be aware to protocols employed at other layers. This is an important factor when making security actions. For example, an application (Level 7) may not be able to identify the source computer for a communication attempt (Levels 2-3), and therefore, may not be able to provide sufficient security...

Here, Shwed discloses the motivation for network security systems to extract all types of useful data from packets in making a rule selection decision.

Shwed teaches or suggests that packet data which differentiates packets associated with particular network "sessions" would be useful in rule selection.

Shwed discloses (col. 9, line 64 to col. 10, line 65):

...An example of a security rule is implemented using the packet filtering method of the present invention will now be described utilizing as an example the security rule to disallow any Telnet services in the system. Telnet is defined as being a TCP service and having a specific TCP destination port. It will be identified by having a TCP protocol value of 6 in byte location 9 of the packet and by having a destination Telnet protocol number of 23 in byte location 22 of the packet, the value being a two-byte value. This is found in every Telnet request packet.

The first operation in Table 1 is to extract the IP protocol from the packet location 9 and place this in memory. As shown in the "Memory Values" column at the right side of Table 1, this value, 6, is placed at the top of the stack.

Art Unit: 2785

The second operation, the TCP protocol (port) number, which is stated to be 6 above, is placed at the second location in memory. In step 3, the values of the first two layers of the stack are compared, obtaining a positive result...

Here, Shwed teaches that an "Telnet session" is identified by a TCP port number, and that this port number is used, in conjunction with other data, to select the security rules applied to the packet.

Shwed teaches or suggests a rule selection method indistinguishable from Applicant's claimed rule selection method.

Shwed discloses (col. 7, lines 15-56; fig. 5):

...A packet entering the computer on which the packet filter module resides passes through layers 1 and 2 and then is diverted to the packet filter 520, shown on the right hand portion of FIG. 5. The packet is received in block 522. In block 524, the packet is compared with the security rule and a determination is made as to whether or not the packet matches the rule... If the packet does not match the rule, the next rule will be retrieved and the packet examined to see if it matches this rule...

Here, Shwed does not specify that a next rule must be selected according to some fixed order, but rather that a next rule is to be retrieved. One of ordinary skill in the art, at the time the invention was made, would have recognized that Shwed suggests that rules should be retrieved using efficient algorithms, such as hashing functions, in order to achieve fast packet handling.

Shwed teaches or suggests that his security system may be implemented on gateways (firewalls) having multiple hardware interfaces to different networks.

Shwed discloses (col. 3, lines 44-65; fig.2):

...FIG. 2 shows the network of FIG. 1 in which the present invention has been installed...Packet filters 204 have been installed on the system administrator, workstations 104 and gateway 106. Gateway 106 has two such filters, one on its connection to the network and one on its connection to the router 108...

...Packet filters 204 are also installed on the gateway 122 of the remote site 120. One packet filter is installed on the connection between the satellite 112 and the gateway 122, a second packet filter is installed on the connection between the Internet and gateway 122 and a third packet filter is installed on the connection between the gateway and the network...

Here, one of ordinary skill in the art, at the time the invention was made, would have recognized that Shwed teaches or suggests how to implement a "firewall" on gateways, routers, and other

Art Unit: 2785

network equipment by installing packet filters on such equipment and linking a particular packet filter with a particular network hardware interface.

Shwed (U.S. Patent 5,606,668) teaches or suggests each and every limitation of Applicant's independent claim 16.

Shwed teaches or suggests that his security system can be used to create multiple independent security areas (domains).

Shwed discloses (col. 4, lines 43-67; fig.3):

...It is also possible to group various devices together such as, for example, the finance department, the research and development department, the directors of the company. It is thus possible to control data flow not only to individual computers on the network, but also to groups of computers on the network by the appropriate placement of packet filters. This allows the system operator have a great deal of flexibility in the managing of communications on the network. It is possible for example to have the chief financial officer as well as other higher ranking officials of the company such as the CEO and the directors able to communicate directly with the finance group, but filter out communications from other groups. It is also possible to allow electronic mail from all groups but to limit other requests for information to a specified set of computers. This allows the system operator to provide internal as well as external security for the network...

Here Shwed clearly suggests that security areas (domains) can be set up using his security system, and suggests that the motivation for setting up a hierarchy of access privileges would be to enhance the security of a computer network.

Shwed teaches or suggests that his security system can administer security domains independently.

Shwed discloses (col. 4, lines 27-43; fig.3):

...The system administrator enters the security rules via a graphical user interface (GUI)... The system operator can thereby be provided with full reports as to the operation of the network and the success or failure of the security rules. This enables the security administrator to make those changes that are appropriate in order to maintain the security of the network without limiting its connectivity...

Shwed discloses (col. 5, lines 23-56):

...Block 302 is the rule base manager which allows the new security rule to be entered into the system in a graphical manner, thus freeing the system administrator from having to write code to implement a particular security rule or to change a security rule... In addition, a further element which can be specified is the installation location for the rule which specifies on which objects the rule will be enforced (see FIG. 2). If an installation location is not specified, the system places the packet filter module on the communication destination by default. These objects are not necessarily the destination. For example, a communication from the Internet and destined for a local host must necessarily pass through a gateway. Therefore, it is possible to enforce the rule on the gateway, even though the gateway is neither the source nor the destination. By entering the data with acronyms or graphic symbols, each rule can quickly be entered and verified without the need for writing, compiling and checking new code for this purpose. Thus, the system administrator need not be an expert in programming a computer for security purposes...

Here, Shwed discloses that his system allows users unskilled in programming security devices to use his system effectively, and that packet filters, which implement security at specific network objects, can be individually configured with security rules. Shwed suggests to one of ordinary skill in the art that this capability of the Shwed system could have been used advantageously to allow different administrators to configure the security of different parts of the network, thus allowing more detailed and thorough security.

Shwed (U.S. Patent 5,606,668) teaches or suggests each and every limitation of Applicant's dependent claims 2-7, 9-11, 13-15, 18-21, and 23-26.

The arguments applied above to independent claims 1, 8, 12, 16, 17, and 22, and the arguments applied in previous Office Actions, are here incorporated by reference.

For the above reasons, it is believed that the rejections should be sustained.

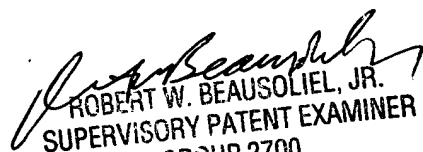
Application/Control Number: 08/927,382
Art Unit: 2785

Page 8

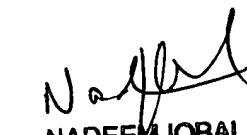
Respectfully submitted,

RGC
September 22, 2000

JOSEPH B RYAN
RYAN AND MASON, L.L.P.
90 FOREST AVENUE
LOCUST VALLEY, NY 11560


ROBERT W. BEAUSOLIEL, JR.
SUPERVISORY PATENT EXAMINER
GROUP 2700


DIEU-MINH LE
PRIMARY EXAMINER
FIRST CONFEREE


NADEEM IQBAL
PRIMARY EXAMINER
CONFEREE